Finite Fields and Their Applications 18 (2012) 993–1012

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Two classes of sequences derived from single cycle T-functions ☆

Wei You, Wen-Feng Qi *, Hong Xu

Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, P.O. Box 1001-745, 450002, Zhengzhou, PR China

ARTICLE INFO

Article history:
Received 20 February 2012
Revised 3 May 2012
Accepted 5 May 2012
Available online 24 May 2012
Communicated by Arne Winterhof

MSC:
11T71
94A60
68P25

Keywords:
Single cycle T-functions
Coordinate sequences
Period
Distribution property
Linear complexity

ABSTRACT

Based on single cycle T-functions over $\mathbb{Z}/(2^n)$, two classes of pseudorandom sequences are proposed in this paper. The periods of all their coordinate sequences can reach the maximal value 2^n, and the distribution properties and linear complexities of the sequences are also studied. For the first class of sequences, it is shown that the less significant half of the coordinate sequences are uniformly distributed over $\mathbb{F}_2$ and the exact linear complexities are also derived. For the second class of sequences, lower bounds on the linear complexities of their coordinate sequences are given.

1. Introduction

T-functions are a class of cryptographic primitives introduced by Klimov and Shamir [1–5], which are well suited for the design of stream ciphers. TSC [6,7], ABC [8] and Mir [9], the eSTREAM candidates, all use T-functions as driving blocks. They are efficient because of using operations available in modern processors, including logical operations (XOR, AND, OR, NOT) and algebraic operations

☆ This work was supported by the NSF of China under Grant Nos. 61070178 and 61100200.

* Corresponding author.
E-mail addresses: youwei1102@163.com (W. You), wenfeng.qi@263.net (W.-F. Qi), xuhong0504@163.com (H. Xu).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2012.05.003

(addition, multiplication, subtraction, negation) modulo 2^n, and their security mainly relies on the mixture of logical and algebraic operations.

The research performed so far focuses on single cycle T-functions, which can generate sequences of period 2^n (see Definition 2.2). However, the period of the jth coordinate sequence is equal to 2^{j+1}, which is far from 2^n except for the $(n-1)$th coordinate sequence. Therefore, these less significant bits should be discarded or masked in applications. In [10], Mitra and Sarkar suggested to use conjugate permutations to improve the intermixing of the most and least significant bits, and in [11], Kolokotronis presented a class of linear permutations, by which the periods of all the coordinate sequences generated by the conjugate of single cycle T-functions can reach the maximal value.

In this paper, by rearranging the coordinate sequences generated by two single cycle T-functions, we propose another two classes of sequences such that the periods of all the coordinate sequences can reach the maximal value 2^n. For an n-bit integer $\boldsymbol{x} = (x_{n-1}, x_{n-2}, \ldots, x_0)$, let $\sigma(\boldsymbol{x}) = (x_{\frac{n}{2}}, \ldots, x_{n-1}, x_{\frac{n}{2}-1}, \ldots, x_0)$ and $\tau(\boldsymbol{x}) = (x_{\frac{n}{2}-1}, \ldots, x_0, x_{\frac{n}{2}}, \ldots, x_{n-1})$ be two bit-permutations of $\boldsymbol{x}$. Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ and $\underline{\boldsymbol{y}} = (\boldsymbol{y}_0, \boldsymbol{y}_1, \ldots)$ be two sequences over $\mathbb{Z}/(2^n)$ generated by single cycle T-functions $f(\boldsymbol{x})$ with initial state $\boldsymbol{x}_0$ and $g(\boldsymbol{y})$ with initial state $\boldsymbol{y}_0$, respectively. The first class of sequences is defined by $\underline{\boldsymbol{z}} = (\boldsymbol{z}_0, \boldsymbol{z}_1, \ldots)$, where $\boldsymbol{z}_i = \sigma(\boldsymbol{x}_i) + \tau(\boldsymbol{y}_i) \pmod{2^n}$, $i \geqslant 0$. We also show that the less significant half of the coordinate sequences of $\underline{\boldsymbol{z}}$ are uniformly distributed over $\mathbb{F}_2$, and derive their exact linear complexities. To obtain sequences with good pseudorandom properties, we further propose the second class of sequences defined by $\underline{\boldsymbol{u}} = (\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots)$, where $\boldsymbol{u}_i = (\sigma(\boldsymbol{x}_i) + \tau(\boldsymbol{y}_i) \bmod 2^n) + \lfloor(\sigma(\boldsymbol{x}_i) + \tau(\boldsymbol{y}_i))/2^n\rfloor$, $i \geqslant 0$. Lower bounds on the linear complexities of their coordinate sequences are given. Although we focus on single word T-functions in this paper, similar conclusions can also be drawn for multiword T-functions.

2. Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of two elements. A word $\boldsymbol{x} \in \mathbb{F}_2^n$ is a vector $\boldsymbol{x} = (x_{n-1}, x_{n-2}, \ldots, x_0)$ of length n, where x_j denotes its jth bit and x_{n-1} is the most significant bit of $\boldsymbol{x}$. Every word $\boldsymbol{x}$ can also be associated with an integer $x = \sum_{j=0}^{n-1} x_j 2^j$ in the residue class ring $\mathbb{Z}/(2^n)$ of integers modulo 2^n.

In the following, we always use the binary form $(x_{n-1}, x_{n-2}, \ldots, x_0)$ to represent an n-bit integer $x = \sum_{j=0}^{n-1} x_j 2^j$ over $\mathbb{Z}/(2^n)$. To avoid confusion with the usual sum, we denote the sum over $\mathbb{F}_2$ by $\oplus$.

Definition 2.1. (See [1].) A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, with $f(\boldsymbol{x}) = \boldsymbol{y}$, is said to be a triangular function (or T-function in short) if the jth bit of the output y_j only depends on the lower input bits $x_0, x_1, \ldots, x_j$, for $0 \leqslant j \leqslant n-1$.

Remark 2.1. Since an n-bit integer $x = \sum_{j=0}^{n-1} x_j 2^j$ over $\mathbb{Z}/(2^n)$ can also be written as $(x_{n-1}, x_{n-2}, \ldots, x_0)$ in its binary form, $f(\boldsymbol{x})$ can also be taken as a T-function from $\mathbb{Z}/(2^n)$ to $\mathbb{Z}/(2^n)$.

Definition 2.2. (See [1].) Let $f : \mathbb{Z}/(2^n) \to \mathbb{Z}/(2^n)$ be a T-function. Given initial state $\boldsymbol{x}_0 = (x_{0,n-1}, x_{0,n-2}, \ldots, x_{0,0}) \in \mathbb{Z}/(2^n)$, the transition from a state $\boldsymbol{x}_i$ to a state $\boldsymbol{x}_{i+1}$ is defined by $\boldsymbol{x}_i \to \boldsymbol{x}_{i+1} = f(\boldsymbol{x}_i)$ for all $i \geqslant 0$. We denote by $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ the state sequence. If $\underline{\boldsymbol{x}}$ has period $per(\underline{\boldsymbol{x}}) = 2^n$, then $f(\boldsymbol{x})$ is called a single cycle T-function and the sequence $\underline{\boldsymbol{x}}$ is said to be generated by $f(\boldsymbol{x})$ and initial state $\boldsymbol{x}_0$.

Remark 2.2. It is clear that such single cycle T-function $f(\boldsymbol{x})$ actually defines a special kind of permutation over $\mathbb{Z}/(2^n)$.

Definition 2.3. (See [2].) Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ be a sequence over $\mathbb{Z}/(2^n)$, where $\boldsymbol{x}_i = (x_{i,n-1}, x_{i,n-2}, \ldots, x_{i,0})$ for all $i \geqslant 0$. Then for $0 \leqslant j \leqslant n-1$, the sequence $\underline{x}_j = (x_{0,j}, x_{1,j}, \ldots)$ is called the jth coordinate sequence of $\underline{\boldsymbol{x}}$.

Lemma 2.1. *(See [2].) Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ be a sequence generated by a single cycle T-function $f(\boldsymbol{x})$ and an initial state $\boldsymbol{x}_0$. Then for $0 \leqslant j \leqslant n-1$, the jth coordinate sequence of $\underline{\boldsymbol{x}}$ has period $per(\underline{x}_j) = 2^{j+1}$. Moreover,*

for $0 \leqslant j \leqslant n-1$, the second half of one period of the sequence $\underline{x}_j$ is the bitwise complement of the first half, i.e., $x_{i+2^j,j} = x_{i,j} \oplus 1$ for $i \geqslant 0$.

From Lemma 2.1, we can easily derive the following result.

Property 2.1. *Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ be a sequence generated by a single cycle T-function $f(\boldsymbol{x})$ and an initial state $\boldsymbol{x}_0$. Then for any fixed integer k, $0 \leqslant k \leqslant n$, we have*

$$x_{i,j} \oplus x_{i+2^{n-k},j} = \begin{cases} 0, & \text{if } 0 \leqslant j < n-k, \\ 1, & \text{if } j = n-k, \\ *, & \text{if } n-k < j < n, \end{cases}$$

where $* \in \mathbb{F}_2$ denotes an arbitrary value depending on i for each $n-k < j < n$.

Lemma 2.2. *(See [11].) Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ be a sequence generated by a single cycle T-function $f(\boldsymbol{x})$ and an initial state $\boldsymbol{x}_0$. Then for $0 \leqslant j \leqslant n-1$, the jth coordinate sequence of $\underline{\boldsymbol{x}}$ has linear complexity $LC(\underline{x}_j) = 2^j + 1$, and the minimal polynomial of the sequence $\underline{x}_j$ is*

$$h_j(x) = (1 \oplus x)^{2^j+1}.$$

Let $\boldsymbol{a} = (a_{n-1}, a_{n-2}, \ldots, a_0)$ and $\boldsymbol{b} = (b_{n-1}, b_{n-2}, \ldots, b_0)$ be two n-bit integers. Then the sum $\boldsymbol{a} + \boldsymbol{b}$ is an $(n+1)$-bit integer whose binary form is given in the following lemma.

Lemma 2.3. *(See [12].) Let $\boldsymbol{a} = (a_{n-1}, a_{n-2}, \ldots, a_0)$, $\boldsymbol{b} = (b_{n-1}, b_{n-2}, \ldots, b_0)$, and $\boldsymbol{a} + \boldsymbol{b} = (c_n, c_{n-1}, \ldots, c_0)$. Then*

$$\begin{aligned} c_0 &= a_0 \oplus b_0, \\ c_j &= a_j \oplus b_j \oplus \left(\bigoplus_{t=0}^{j-1} a_t b_t \prod_{s=t+1}^{j-1} (a_s \oplus b_s) \right), \quad 1 \leqslant j \leqslant n-1, \\ c_n &= \bigoplus_{t=0}^{n-1} a_t b_t \prod_{s=t+1}^{n-1} (a_s \oplus b_s), \end{aligned}$$

where we define $\prod_{s=j}^{j-1} (a_s \oplus b_s) = 1$.

In the following, we always suppose that n is an even integer, $f(\boldsymbol{x})$ and $g(\boldsymbol{y})$ are T-functions over $\mathbb{Z}/(2^n)$, and $\prod_{i \in \varnothing} = 1$ for the empty set $\varnothing$.

3. The first class of sequences

Let $\boldsymbol{x} = (x_{n-1}, x_{n-2}, \ldots, x_0)$ be an n-bit integer, and $\sigma(\boldsymbol{x}) = (x_{\frac{n}{2}}, \ldots, x_{n-1}, x_{\frac{n}{2}-1}, \ldots, x_0)$ and $\tau(\boldsymbol{x}) = (x_{\frac{n}{2}-1}, \ldots, x_0, x_{\frac{n}{2}}, \ldots, x_{n-1})$ be two bit-permutations of $\boldsymbol{x}$. Equivalently, we may write $\boldsymbol{x} = \sum_{j=0}^{n-1} x_j 2^j$ and

$$\sigma(\boldsymbol{x}) = \left(\sum_{j=\frac{n}{2}}^{n-1} x_j 2^{\frac{3n}{2}-j-1} \right) + \left(\sum_{j=0}^{\frac{n}{2}-1} x_j 2^j \right), \qquad \tau(\boldsymbol{x}) = \left(\sum_{j=0}^{\frac{n}{2}-1} x_j 2^{\frac{n}{2}+j} \right) + \left(\sum_{j=\frac{n}{2}}^{n-1} x_j 2^{n-j-1} \right).$$

Definition 3.1. Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ be a sequence generated by the single cycle T-function $f(\boldsymbol{x})$ and the initial state $\boldsymbol{x}_0$, and $\underline{\boldsymbol{y}} = (\boldsymbol{y}_0, \boldsymbol{y}_1, \ldots)$ be a sequence generated by the single cycle T-function $g(\boldsymbol{y})$ and the initial state $\boldsymbol{y}_0$. For all $i \geqslant 0$, set $\boldsymbol{z}_i = \sigma(\boldsymbol{x}_i) + \tau(\boldsymbol{y}_i) \pmod{2^n}$. Then the sequence $\underline{\boldsymbol{z}} = (\boldsymbol{z}_0, \boldsymbol{z}_1, \ldots)$ is said to be generated by 4-tuple $(f(\boldsymbol{x}), g(\boldsymbol{y}), \boldsymbol{x}_0, \boldsymbol{y}_0)$.

It is clear that the sequence $\underline{\boldsymbol{z}}$ is obtained by simply mixing the most and least significant coordinate sequences generated by two single cycle T-functions. In order to further study their cryptographic properties, we first present three lemmas.

Lemma 3.1. *Let $\underline{\boldsymbol{z}} = (\boldsymbol{z}_0, \boldsymbol{z}_1, \ldots)$ be a sequence generated by 4-tuple $(f(\boldsymbol{x}), g(\boldsymbol{y}), \boldsymbol{x}_0, \boldsymbol{y}_0)$. Then for all $i \geqslant 0$, we have*

$$z_{i,0} = x_{i,0} \oplus y_{i,n-1}. \tag{1a}$$

$$z_{i,j} = x_{i,j} \oplus y_{i,n-j-1} \oplus \left(\bigoplus_{t=0}^{j-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{j-1} (x_{i,s} \oplus y_{i,n-s-1}) \right), \quad 1 \leqslant j \leqslant \frac{n}{2} - 1. \tag{1b}$$

$$z_{i,\frac{n}{2}} = x_{i,n-1} \oplus y_{i,0} \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right). \tag{1c}$$

$$\begin{aligned} z_{i,j} = {} & x_{i,\frac{3n}{2}-j-1} \oplus y_{i,j-\frac{n}{2}} \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \prod_{s=\frac{3n}{2}-j}^{n-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\ & \oplus \left(\bigoplus_{t=0}^{j-\frac{n}{2}-1} x_{i,n-t-1} y_{i,t} \prod_{s=t+1}^{j-\frac{n}{2}-1} (x_{i,n-s-1} \oplus y_{i,s}) \right), \quad \frac{n}{2} + 1 \leqslant j \leqslant n-1. \end{aligned} \tag{1d}$$

Proof. According to the definition of the sequence $\underline{\boldsymbol{z}}$, the result can be obtained easily from Lemma 2.3. □

Similarly to (1d), let

$$\begin{aligned} z_{i,n} = {} & x_{i,\frac{n}{2}-1} \oplus y_{i,\frac{n}{2}} \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{n-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\ & \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,n-t-1} y_{i,t} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,n-s-1} \oplus y_{i,s}) \right). \end{aligned} \tag{1e}$$

Then the following lemma holds.

Lemma 3.2. *Let $z_{i,j}$ be defined as above, where $0 \leqslant j \leqslant n$. Then for all $i \geqslant 0$, we have*

$$z_{i,0} \oplus z_{i+2^{n-1},0} = 1. \tag{2a}$$

$$z_{i,j} \oplus z_{i+2^{n-1},j} = x_{i,0} \prod_{s=1}^{j-1} (x_{i,s} \oplus y_{i,n-s-1}), \quad 1 \leqslant j \leqslant \frac{n}{2} - 1. \tag{2b}$$

$$z_{i,\frac{n}{2}} \oplus z_{i+2^{n-1},\frac{n}{2}} = 1 \oplus x_{i,0} \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}). \tag{2c}$$

$$z_{i,j} \oplus z_{i+2^{n-1},j} = \xi_i \cdot \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i,s} \oplus y_{i,n-s-1}), \quad \frac{n}{2}+1 \leqslant j \leqslant n, \tag{2d}$$

where

$$\xi_i = x_{i,\frac{n}{2}-1} y_{i,\frac{n}{2}} \oplus y_{i,0} \oplus (x_{i,\frac{n}{2}-1} \oplus y_{i,\frac{n}{2}}) \cdot \zeta_i,$$

$$\zeta_i = x_{i,0}(x_{i,n-1} \oplus y_{i,n-1} \oplus y_{i,0} \oplus 1) \prod_{s=1}^{\frac{n}{2}-2} (x_{i,s} \oplus y_{i,n-s-1}) \oplus \left(\bigoplus_{t=1}^{\frac{n}{2}-2} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-2} (x_{i,s} \oplus y_{i,n-s-1}) \right).$$

Proof. The proof of Lemma 3.2 is presented in Appendix A for completeness. □

Lemma 3.3. *Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ be a sequence generated by the single cycle T-function $f(\boldsymbol{x})$ and the initial state $\boldsymbol{x}_0$, and $\underline{\boldsymbol{y}} = (\boldsymbol{y}_0, \boldsymbol{y}_1, \ldots)$ be a sequence generated by the single cycle T-function $g(\boldsymbol{y})$ and the initial state $\boldsymbol{y}_0$. Then there exists nonnegative integer i^* such that the following equalities hold (for the three equalities, i^* is not necessarily the same).*

$$x_{i^*,0} \prod_{s=1}^{\frac{n}{2}-1} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1. \tag{3a}$$

$$(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,0})(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,\frac{n}{2}} \oplus 1)(x_{i^*,0} \oplus y_{i^*,n-1}) \prod_{s=\frac{n}{2}+1}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1. \tag{3b}$$

$$x_{i^*,0}(y_{i^*,\frac{n}{2}-1} \oplus 1)(x_{i^*,\frac{n}{2}} \oplus 1)(x_{i^*,0} \oplus y_{i^*,n-1}) \prod_{s=1}^{\frac{n}{2}-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1. \tag{3c}$$

Proof. The proof of Lemma 3.3 is presented in Appendix B for completeness. □

3.1. The periods of the coordinate sequences of $\underline{\boldsymbol{z}}$

Theorem 3.1. *Let $\underline{\boldsymbol{z}} = (\boldsymbol{z}_0, \boldsymbol{z}_1, \ldots)$ be a sequence generated by 4-tuple $(f(\boldsymbol{x}), g(\boldsymbol{y}), \boldsymbol{x}_0, \boldsymbol{y}_0)$. Then for all $0 \leqslant j \leqslant n-1$, the jth coordinate sequence of $\underline{\boldsymbol{z}}$ has period $per(\underline{z}_j) = 2^n$.*

Proof. From the definition of the sequence $\underline{\boldsymbol{z}}$ we know that $per(\underline{\boldsymbol{z}}) \mid 2^n$, and so it suffices to show that for each $0 \leqslant j \leqslant n-1$, there exists nonnegative integer i^* such that $z_{i^*,j} \oplus z_{i^*+2^{n-1},j} = 1$ (i^* is not necessarily the same for all j, we use it uniformly for convenience).

(i) If $j = 0$, by Lemma 3.2(2a) we know there exists integer $i^* \geqslant 0$ such that

$$z_{i^*,0} \oplus z_{i^*+2^{n-1},0} = 1.$$

(ii) If $1 \leqslant j \leqslant \frac{n}{2} - 1$, by Lemma 3.3(3a) we know there exists integer $i^* \geqslant 0$ such that

$$x_{i^*,0} \prod_{s=1}^{\frac{n}{2}-1} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

Then from Lemma 3.2(2b) we have

$$z_{i^*,j} \oplus z_{i^*+2^{n-1},j} = x_{i^*,0} \prod_{s=1}^{j-1} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

(iii) If $j = \frac{n}{2}$, since $per(\underline{x}_0) = 2$, there exists integer $i^* \geqslant 0$ such that $x_{i^*,0} = 0$. Thus from Lemma 3.2(2c) we have

$$z_{i^*,\frac{n}{2}} \oplus z_{i^*+2^{n-1},\frac{n}{2}} = 1 \oplus x_{i^*,0} \prod_{s=1}^{\frac{n}{2}-1} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

(iv) If $\frac{n}{2} + 1 \leqslant j \leqslant n - 1$, by Lemma 3.3(3b) we know there exists integer $i^* \geqslant 0$ such that

$$(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,0})(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,\frac{n}{2}} \oplus 1)(x_{i^*,0} \oplus y_{i^*,n-1}) \prod_{s=\frac{n}{2}+1}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

That is,

$$x_{i^*,\frac{n}{2}-1} = y_{i^*,\frac{n}{2}} = y_{i^*,0} \oplus 1 \quad \text{and} \quad \prod_{s=\frac{n}{2}+1}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

Thus

$$\prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1, \quad \frac{n}{2} + 1 \leqslant j \leqslant n - 1.$$

Therefore, it follows from Lemma 3.2(2d) that

$$\begin{aligned} z_{i^*,j} \oplus z_{i^*+2^{n-1},j} &= \xi_{i^*} \cdot \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = \xi_{i^*} = x_{i^*,\frac{n}{2}-1} y_{i^*,\frac{n}{2}} \oplus y_{i^*,0} \\ &= x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,0} = 1. \end{aligned}$$

This completes the proof. □

3.2. The distribution properties of the coordinate sequences of $\underline{\boldsymbol{z}}$

Theorem 3.2. *Let $\underline{\boldsymbol{z}} = (\boldsymbol{z}_0, \boldsymbol{z}_1, \ldots)$ be a sequence generated by 4-tuple $(f(\boldsymbol{x}), g(\boldsymbol{y}), \boldsymbol{x}_0, \boldsymbol{y}_0)$. Then for $0 \leqslant j \leqslant \frac{n}{2} - 1$, the number of 0's and the number of 1's occurring in one period of the jth coordinate sequence of $\underline{\boldsymbol{z}}$ are equal.*

Proof. For an n-bit integer $\boldsymbol{w} = (w_{n-1}, w_{n-2}, \ldots, w_0)$, let

$$h(\boldsymbol{w}) = (w_{\frac{n}{2}}, w_{\frac{n}{2}+1}, \ldots, w_{n-1}) \quad \text{and} \quad l(\boldsymbol{w}) = (w_{\frac{n}{2}-1}, w_{\frac{n}{2}-2}, \ldots, w_0).$$

Then from the definition of the sequence $\underline{\boldsymbol{z}}$ we have

$$l(\boldsymbol{z}_i) = l(\boldsymbol{x}_i) + h(\boldsymbol{y}_i) \left(\mathrm{mod}\, 2^{\frac{n}{2}}\right), \quad i \geqslant 0.$$

On one hand, since the sequence $\underline{\boldsymbol{x}} = \{\boldsymbol{x}_i\}_{i\geqslant 0}$ is generated by the single cycle T-function $f(\boldsymbol{x})$ and the initial state $\boldsymbol{x}_0$, by Property 2.1 we know that

$$l(\boldsymbol{x}_i) = l(\boldsymbol{x}_{i+2^{n/2}}), \quad i \geqslant 0. \tag{4a}$$

On the other hand, since the sequence $\underline{\boldsymbol{y}} = \{\boldsymbol{y}_i\}_{i\geqslant 0}$ is generated by the single cycle T-function $g(\boldsymbol{y})$ and the initial state $\boldsymbol{y}_0$, we can claim that for any integers $i \geqslant 0$ and $k \in \{1, 2, \ldots, 2^{n/2} - 1\}$, we have

$$h(\boldsymbol{y}_i) \neq h(\boldsymbol{y}_{i+k\cdot 2^{n/2}}). \tag{4b}$$

Otherwise, suppose there exist nonnegative integers i^* and k^*, where $k^* \in \{1, 2, \ldots, 2^{n/2} - 1\}$, such that $h(\boldsymbol{y}_{i^*}) = h(\boldsymbol{y}_{i^*+k^*\cdot 2^{n/2}})$. Then from (4a) we know $l(\boldsymbol{y}_{i^*}) = l(\boldsymbol{y}_{i^*+k^*\cdot 2^{n/2}})$. Hence $\boldsymbol{y}_{i^*} = \boldsymbol{y}_{i^*+k^*\cdot 2^{n/2}}$. This is in contradiction with the condition that the period of $\underline{\boldsymbol{y}}$ is $per(\underline{\boldsymbol{y}}) = 2^n$.

It follows from (4b) that for any fixed $i \geqslant 0$,

$$\left\{h(\boldsymbol{y}_{i+k\cdot 2^{n/2}}) \,\middle|\, k = 0, 1, \ldots, 2^{\frac{n}{2}} - 1\right\} = \left\{0, 1, \ldots, 2^{\frac{n}{2}} - 1\right\}.$$

Then by (4a) we know that for any fixed $i \geqslant 0$,

$$\begin{aligned}\left\{l(\boldsymbol{z}_{i+k\cdot 2^{n/2}}) \,\middle|\, k = 0, 1, \ldots, 2^{\frac{n}{2}} - 1\right\} &= \left\{l(\boldsymbol{x}_{i+k\cdot 2^{n/2}}) + h(\boldsymbol{y}_{i+k\cdot 2^{n/2}}) \bmod 2^{\frac{n}{2}} \,\middle|\, k = 0, 1, \ldots, 2^{\frac{n}{2}} - 1\right\} \\ &= \left\{l(\boldsymbol{x}_i) + h(\boldsymbol{y}_{i+k\cdot 2^{n/2}}) \bmod 2^{\frac{n}{2}} \,\middle|\, k = 0, 1, \ldots, 2^{\frac{n}{2}} - 1\right\} \\ &= \left\{0, 1, \ldots, 2^{\frac{n}{2}} - 1\right\}.\end{aligned}$$

Thus, if i runs through the set $\{0, 1, \ldots, 2^n - 1\}$, then $l(\boldsymbol{z}_i)$ runs through the set $\{0, 1, \ldots, 2^{\frac{n}{2}} - 1\}$ just $2^{\frac{n}{2}}$ times. Therefore, for $0 \leqslant j \leqslant \frac{n}{2} - 1$, the number of 0's and the number of 1's occurring in one period of the sequence $\underline{z}_j$ are equal. □

3.3. The linear complexities of the coordinate sequences of $\underline{\boldsymbol{z}}$

Theorem 3.3. *Let $\underline{\boldsymbol{z}} = (\boldsymbol{z}_0, \boldsymbol{z}_1, \ldots)$ be a sequence generated by 4-tuple $(f(\boldsymbol{x}), g(\boldsymbol{y}), \boldsymbol{x}_0, \boldsymbol{y}_0)$. Then for $0 \leqslant j \leqslant \frac{n}{2} - 1$, the linear complexity of the jth coordinate sequence of $\underline{\boldsymbol{z}}$ is as follows:*

$$LC(\underline{z}_j) = \begin{cases} 1 + 2^{n-1}, & \text{if } j = 0, \\ 2 + \sum_{t=1}^{j} 2^{n-t}, & \text{if } 0 < j < \frac{n}{2}. \end{cases}$$

Proof. From Theorem 3.1 we know that

$$per(\underline{z}_j) = 2^n, \quad 0 \leqslant j \leqslant \frac{n}{2} - 1.$$

Then we have

$$2^{n-1} + 1 \leqslant LC(\underline{z}_j) \leqslant 2^n, \quad 0 \leqslant j \leqslant \frac{n}{2} - 1. \tag{5}$$

(i) If $j = 0$, then by Lemma 3.1(1a) we have $\underline{z}_0 = \underline{x}_0 \oplus \underline{y}_{n-1}$. On the other hand, from Lemma 2.2 we have

$$(1 \oplus x)^2 \underline{x}_0 = \underline{0} \quad \text{and} \quad (1 \oplus x)^{2^{n-1}+1} \underline{y}_{n-1} = \underline{0}.$$

Thus

$$(1 \oplus x)^{2^{n-1}+1} \underline{z}_0 = \underline{0}.$$

It follows from (5) that

$$LC(\underline{z}_0) = 2^{n-1} + 1.$$

(ii) If $j = 1$, then by Lemma 3.1(1b) we have $\underline{z}_1 = \underline{x}_1 \oplus \underline{y}_{n-2} \oplus \underline{x}_0 \underline{y}_{n-1}$. On the other hand, from Lemma 2.2 we have

$$(1 \oplus x)^3 \underline{x}_1 = \underline{0}, \qquad (1 \oplus x)^{2^{n-2}+1} \underline{y}_{n-2} = \underline{0}, \quad \text{and} \quad (1 \oplus x)^{2^{n-1}+1} \underline{y}_{n-1} = \underline{0}.$$

Next we shall show that

$$(1 \oplus x)^{2^{n-1}+2} (\underline{x}_0 \underline{y}_{n-1}) = \underline{0} \quad \text{and} \quad (1 \oplus x)^{2^{n-1}+1} (\underline{x}_0 \underline{y}_{n-1}) \neq \underline{0}.$$

In fact, combining with Property 2.1 we know that for all $i \geqslant 0$,

$$\begin{aligned} &x_{i,0} y_{i,n-1} \oplus x_{i+2,0} y_{i+2,n-1} \oplus x_{i+2^{n-1},0} y_{i+2^{n-1},n-1} \oplus x_{i+2^{n-1}+2,0} y_{i+2^{n-1}+2,n-1} \\ &\quad = x_{i,0}(y_{i,n-1} \oplus y_{i+2,n-1} \oplus y_{i+2^{n-1},n-1} \oplus y_{i+2^{n-1}+2,n-1}) = 0 \end{aligned}$$

and

$$\begin{aligned} &x_{i,0} y_{i,n-1} \oplus x_{i+1,0} y_{i+1,n-1} \oplus x_{i+2^{n-1},0} y_{i+2^{n-1},n-1} \oplus x_{i+2^{n-1}+1,0} y_{i+2^{n-1}+1,n-1} \\ &\quad = x_{i,0}(y_{i,n-1} \oplus y_{i+2^{n-1},n-1}) \oplus x_{i+1,0}(y_{i+1,n-1} \oplus y_{i+2^{n-1}+1,n-1}) = x_{i,0} \oplus x_{i+1,0} = 1. \end{aligned}$$

That is,

$$(1 \oplus x)^{2^{n-1}+2} (\underline{x}_0 \underline{y}_{n-1}) = \underline{0} \quad \text{and} \quad (1 \oplus x)^{2^{n-1}+1} (\underline{x}_0 \underline{y}_{n-1}) = \underline{1}.$$

Thus

$$(1 \oplus x)^{2^{n-1}+2} \underline{z}_1 = \underline{0} \quad \text{and} \quad (1 \oplus x)^{2^{n-1}+1} \underline{z}_1 = \underline{1}.$$

Hence

$$LC(\underline{z}_1) = 2^{n-1} + 2.$$

(iii) If $2 \leqslant j \leqslant \frac{n}{2} - 1$, then by Lemma 3.1(1b) we know that

$$\underline{z}_j = \underline{x}_j \oplus \underline{y}_{n-j-1} \oplus \left(\bigoplus_{t=0}^{j-1} \underline{x}_t \underline{y}_{n-t-1} \prod_{s=t+1}^{j-1} (\underline{x}_s \oplus \underline{y}_{n-s-1}) \right).$$

Hence, we have

$$\underline{z}_j = \underline{x}_{j-1} \oplus \underline{x}_j \oplus \underline{y}_{n-j-1} \oplus \underline{y}_{n-j} \oplus \underline{z}_{j-1}(\underline{x}_{j-1} \oplus \underline{y}_{n-j}) \oplus \underline{x}_{j-1}\underline{y}_{n-j}.$$

On the other hand, from Lemmas 2.1 and 2.2 we know that

$$(1 \oplus x)^{2^{n-1}} (\underline{x}_{j-1} \oplus \underline{x}_j \oplus \underline{y}_{n-j-1} \oplus \underline{y}_{n-j} \oplus \underline{x}_{j-1}\underline{y}_{n-j}) = \underline{0}.$$

Therefore, it follows from (5) that

$$LC(\underline{z}_j) = LC\big(\underline{z}_{j-1}(\underline{x}_{j-1} \oplus \underline{y}_{n-j})\big), \quad j \geqslant 2. \tag{6a}$$

Next we shall show the following equation holds by induction on j.

$$LC\big(\underline{z}_{j-1}(\underline{x}_{j-1} \oplus \underline{y}_{n-j})\big) = LC(\underline{z}_{j-1}) + 2^{n-j}. \tag{6b}$$

1) When $j = 2$, since the minimal polynomial of the sequence $\underline{z}_1$ is $h(x) = (1 \oplus x)^{2^{n-1}+2}$, by Property 2.1 we know that for all $i \geqslant 0$,

$$\begin{aligned}
&z_{i+2^{n-1}+2^{n-2}+2,1} y_{i+2^{n-1}+2^{n-2}+2,n-2} \oplus z_{i+2^{n-1}+2^{n-2},1} y_{i+2^{n-1}+2^{n-2},n-2} \\
&\quad \oplus z_{i+2^{n-1}+2,1} y_{i+2^{n-1}+2,n-2} \oplus z_{i+2^{n-1},1} y_{i+2^{n-1},n-2} \oplus z_{i+2^{n-2}+2,1} y_{i+2^{n-2}+2,n-2} \\
&\quad \oplus z_{i+2^{n-2},1} y_{i+2^{n-2},n-2} \oplus z_{i+2,1} y_{i+2,n-2} \oplus z_{i,1} y_{i,n-2} \\
&= y_{i+2,n-2}(z_{i+2^{n-1}+2^{n-2}+2,1} \oplus z_{i+2^{n-1}+2,1} \oplus z_{i+2^{n-2}+2,1} \oplus z_{i+2,1}) \\
&\quad \oplus y_{i,n-2}(z_{i+2^{n-1}+2^{n-2},1} \oplus z_{i+2^{n-1},1} \oplus z_{i+2^{n-2},1} \oplus z_{i,1}) \\
&\quad \oplus (z_{i+2^{n-1}+2^{n-2}+2,1} \oplus z_{i+2^{n-1}+2^{n-2},1} \oplus z_{i+2^{n-2}+2,1} \oplus z_{i+2^{n-2},1}) \\
&= 0.
\end{aligned}$$

That is,

$$(1 \oplus x)^{2^{n-1}+2^{n-2}+2} (\underline{z}_1 \underline{y}_{n-2}) = \underline{0}.$$

Similarly, we can prove

$$(1 \oplus x)^{2^{n-1}+2^{n-2}+2} \big(\underline{z}_1(\underline{x}_1 \oplus \underline{y}_{n-2})\big) = \underline{0} \quad \text{and} \quad (1 \oplus x)^{2^{n-1}+2^{n-2}+1} \big(\underline{z}_1(\underline{x}_1 \oplus \underline{y}_{n-2})\big) = \underline{1}.$$

Then we have

$$LC\big(\underline{z}_1(\underline{x}_1 \oplus \underline{y}_{n-2})\big) = 2^{n-1} + 2^{n-2} + 2 = LC(\underline{z}_1) + 2^{n-2}.$$

Thus, (6b) holds for $j = 2$.

2) Suppose (6b) holds for all $j \leqslant k < \frac{n}{2} - 1$. Then by (6a) we have

$$LC(\underline{z}_j) = LC\big(\underline{z}_{j-1}(\underline{x}_{j-1} \oplus \underline{y}_{n-j})\big) = LC(\underline{z}_{j-1}) + 2^{n-j}, \quad 2 \leqslant j \leqslant k.$$

Hence,

$$LC(\underline{z}_k) = 2 + \sum_{t=1}^{k} 2^{n-t}.$$

Similarly to 1) we can show that

$$LC\big(\underline{z}_k(\underline{x}_k \oplus \underline{y}_{n-k-1})\big) = 2 + \sum_{t=1}^{k+1} 2^{n-t} = LC(\underline{z}_k) + 2^{n-k-1}.$$

Thus, (6b) holds for $j = k + 1$.

Therefore, Eq. (6b) holds for all integers $j \geqslant 2$. Combining with (6a) and (6b), we have

$$LC(\underline{z}_j) = 2 + \sum_{t=1}^{j} 2^{n-t}.$$

This completes the proof. □

4. The second class of sequences

Let $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ be a sequence generated by the single cycle T-function $f(\boldsymbol{x})$ and the initial state $\boldsymbol{x}_0$, and $\underline{\boldsymbol{y}} = (\boldsymbol{y}_0, \boldsymbol{y}_1, \ldots)$ be a sequence generated by the single cycle T-function $g(\boldsymbol{y})$ and the initial state $\boldsymbol{y}_0$. For all $i \geqslant 0$, set

$$\boldsymbol{u}_i = \big(\sigma(\boldsymbol{x}_i) + \tau(\boldsymbol{y}_i) \bmod 2^n\big) + \big\lfloor \big(\sigma(\boldsymbol{x}_i) + \tau(\boldsymbol{y}_i)\big)/2^n \big\rfloor, \tag{7a}$$

where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x.

Denote $\eta_i = \lfloor (\sigma(\boldsymbol{x}_i) + \tau(\boldsymbol{y}_i))/2^n \rfloor$. It is clear that $\eta_i \in \{0, 1\}$, and from Lemma 2.3 we know that

$$\eta_i = \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,t}\, y_{i,n-t-1} \prod_{s=t+1}^{n-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,n-t-1}\, y_{i,t} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,n-s-1} \oplus y_{i,s}) \right). \tag{7b}$$

It follows from (1e) that $\eta_i = z_{i,n} \oplus x_{i,\frac{n}{2}-1} \oplus y_{i,\frac{n}{2}}$. By using Lemma 3.2(2d) and Property 2.1 we can easily get

$$\eta_i \oplus \eta_{i+2^{n-1}} = \xi_i \cdot \prod_{s=\frac{n}{2}}^{n-2} (x_{i,s} \oplus y_{i,n-s-1}). \tag{7c}$$

On the other hand, from the definition of $\boldsymbol{z}_i$ given in Section 3 we know that

$$\boldsymbol{u}_i = z_{i,n-1}2^{n-1} + z_{i,n-2}2^{n-2} + \cdots + z_{i,1}2 + z_{i,0} + \eta_i.$$

Then from Lemma 2.3 we have

$$u_{i,j} = z_{i,j} \oplus \eta_i \cdot \prod_{t=0}^{j-1} z_{i,t}, \quad 0 \leqslant j \leqslant n-1. \tag{7d}$$

4.1. The periods of the coordinate sequences of $\underline{\boldsymbol{u}}$

Theorem 4.1. *Let the sequence $\underline{\boldsymbol{u}}$ be defined as in (7a). Then for all $0 \leqslant j \leqslant n-1$, the jth coordinate sequence of $\underline{\boldsymbol{u}}$ has period $per(\underline{u}_j) = 2^n$.*

Proof. From the definition of the sequence $\underline{\boldsymbol{u}}$ we know that $per(\underline{\boldsymbol{u}}) \mid 2^n$, and so it suffices to show that for each $0 \leqslant j \leqslant n-1$, there exists nonnegative integer i^* such that $u_{i^*,j} \oplus u_{i^*+2^{n-1},j} = 1$ (i^* is not necessarily the same for all j, we use it uniformly for convenience).

It follows from (7d) that

$$u_{i,j} \oplus u_{i+2^{n-1},j} = z_{i,j} \oplus z_{i+2^{n-1},j} \oplus \eta_i \cdot \prod_{t=0}^{j-1} z_{i,t} \oplus \eta_{i+2^{n-1}} \cdot \prod_{t=0}^{j-1} z_{i+2^{n-1},t}. \tag{8}$$

(i) If $j = 0$, then by Lemma 3.2(2a) we know that

$$u_{i,0} \oplus u_{i+2^{n-1},0} = 1 \oplus \eta_i \oplus \eta_{i+2^{n-1}}.$$

On the other hand, from Property 2.1 we know that there exists integer $i^* \geqslant 0$ such that $x_{i^*,n-2} \oplus y_{i^*,1} = 0$. Thus, from (7c) we have

$$u_{i^*,0} \oplus u_{i^*+2^{n-1},0} = 1 \oplus \eta_{i^*} \oplus \eta_{i^*+2^{n-1}} = 1 \oplus \xi_{i^*} \cdot \prod_{s=\frac{n}{2}}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

(ii) If $1 \leqslant j \leqslant \frac{n}{2} - 1$, then by Lemma 3.3(3c) we know that there exists integer $i^* \geqslant 0$ such that

$$x_{i^*,0}(y_{i^*,\frac{n}{2}-1} \oplus 1)(x_{i^*,\frac{n}{2}} \oplus 1)(x_{i^*,0} \oplus y_{i^*,n-1}) \prod_{s=1}^{\frac{n}{2}-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

That is,

$$x_{i^*,0} \prod_{s=1}^{\frac{n}{2}-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1, \qquad y_{i^*,\frac{n}{2}-1} = x_{i^*,\frac{n}{2}} = 0, \qquad x_{i^*,0} \oplus y_{i^*,n-1} = 1.$$

Then from Lemma 3.2(2b) and (7b) we know that

$$z_{i^*,j} \oplus z_{i^*+2^{n-1},j} = x_{i^*,0} \prod_{s=1}^{j-1} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1 \quad \text{and} \quad \eta_{i^*} = 0.$$

Hence, since $z_{i^*,0} = x_{i^*,0} \oplus y_{i^*,n-1} = 1$, from Lemma 3.2(2a) we have

$$u_{i^*,j} \oplus u_{i^*+2^{n-1},j} = 1 \oplus 0 \oplus 0 = 1.$$

(iii) If $j = \frac{n}{2}$, then by Lemma 3.2(2c) we know that

$$u_{i,\frac{n}{2}} \oplus u_{i+2^{n-1},\frac{n}{2}} = 1 \oplus x_{i,0} \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \oplus \eta_i \cdot \prod_{t=0}^{\frac{n}{2}-1} z_{i,t} \oplus \eta_{i+2^{n-1}} \cdot \prod_{t=0}^{\frac{n}{2}-1} z_{i+2^{n-1},t}.$$

On the other hand, from Property 2.1 we know there exists integer $i^* \geqslant 0$ such that

$$x_{i^*,1} \oplus y_{i^*,n-2} = 0 \quad \text{and} \quad x_{i^*,0} \oplus y_{i^*,n-1} = 1.$$

Then from Lemma 3.1(1a), (1b) we have

$$z_{i^*,0} = x_{i^*,0} \oplus y_{i^*,n-1} = 1$$

and

$$z_{i^*,1} = x_{i^*,1} \oplus y_{i^*,n-2} \oplus x_{i^*,0} y_{i^*,n-1} = 0.$$

Thus from Lemma 3.2(2a) we have

$$u_{i^*,\frac{n}{2}} \oplus u_{i^*+2^{n-1},\frac{n}{2}} = 1 \oplus 0 \oplus 0 \oplus 0 = 1.$$

(iv) If $\frac{n}{2} + 1 \leqslant j \leqslant n-1$, then by Lemma 3.3(3b) we know that there exists integer $i^* \geqslant 0$ such that

$$(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,0})(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,\frac{n}{2}} \oplus 1)(x_{i^*,0} \oplus y_{i^*,n-1}) \prod_{s=\frac{n}{2}+1}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

Similarly to (iv) in the proof of Theorem 3.1 we have $z_{i^*,j} \oplus z_{i^*+2^{n-1},j} = 1$. In addition, if $\prod_{s=1}^{\frac{n}{2}-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1$, then from Lemma 3.1(1b) we have

$$z_{i^*,\frac{n}{2}-1} = x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,\frac{n}{2}} \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-2} x_{i^*,t} y_{i^*,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) \right) = 0 \oplus 0 = 0.$$

Otherwise, let t_0 be the smallest integer $t \in \{1, 2, \ldots, \frac{n}{2} - 2\}$ such that $x_{i^*,t} \oplus y_{i^*,n-t-1} = 0$. Then from Lemma 3.1(1b) we have

$$z_{i^*,t_0} = x_{i^*,t_0} \oplus y_{i^*,n-t_0-1} \oplus \left(\bigoplus_{t=0}^{t_0-1} x_{i^*,t} y_{i^*,n-t-1} \prod_{s=t+1}^{t_0-1} (x_{i^*,s} \oplus y_{i^*,n-s-1}) \right) = 0 \oplus 0 = 0.$$

Hence, since $z_{i^*,0} = x_{i^*,0} \oplus y_{i^*,n-1} = 1$, from Lemma 3.2(2a) we have

$$u_{i^*,j} \oplus u_{i^*+2^{n-1},j} = 1 \oplus 0 \oplus 0 = 1.$$

This completes the proof. □

4.2. The linear complexities of the coordinate sequences of $\underline{\underline{u}}$

Theorem 4.2. *Let the sequence* $\underline{\underline{u}}$ *be defined as in* (7a)*. Then we have*

$$LC(\underline{u}_j) > \begin{cases} 2^{n-1}, & \text{if } j \in \{0, 1, \frac{n}{2}, \frac{n}{2}+1\}, \\ \sum_{t=1}^{j} 2^{n-t}, & \text{if } 1 < j < \frac{n}{2}, \\ \sum_{t=1}^{j-n/2} 2^{n-t}, & \text{if } \frac{n}{2}+1 < j < n. \end{cases}$$

Proof. From Theorem 4.1 we know that

$$per(\underline{u}_j) = 2^n, \quad 0 \leqslant j \leqslant n-1.$$

Then we have

$$2^{n-1}+1 \leqslant LC(\underline{u}_j) \leqslant 2^n, \quad 0 \leqslant j \leqslant n-1.$$

(i) If $1 < j < \frac{n}{2}$, then by Lemma 3.2(2b) and (8) we have

$$\begin{aligned} &\bigoplus_{(k_2,\ldots,k_j)\in\mathbb{F}_2^{j-1}} (u_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j},j} \oplus u_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j}+2^{n-1},j}) \\ &= \bigoplus_{(k_2,\ldots,k_j)\in\mathbb{F}_2^{j-1}} \Bigg(x_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j},0} \prod_{s=1}^{j-1} (x_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j},s} \oplus y_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j},n-s-1}) \\ &\quad \oplus \eta_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j}} \cdot \prod_{t=0}^{j-1} z_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j},t} \\ &\quad \oplus \eta_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j}+2^{n-1}} \cdot \prod_{t=0}^{j-1} z_{i+k_2 2^{n-2}+\cdots+k_j 2^{n-j}+2^{n-1},t} \Bigg). \end{aligned}$$

On the other hand, from Lemma 3.3(3c) we know there exists integer $i^* \geqslant 0$ such that

$$x_{i^*,0}(y_{i^*,\frac{n}{2}-1} \oplus 1)(x_{i^*,\frac{n}{2}} \oplus 1)(x_{i^*,0} \oplus y_{i^*,n-1}) \prod_{s=1}^{\frac{n}{2}-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

Thus

$$x_{i^*,0} \prod_{s=1}^{\frac{n}{2}-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1 \quad \text{and} \quad y_{i^*,\frac{n}{2}-1} = x_{i^*,\frac{n}{2}} = 0.$$

- If $(k_2, \ldots, k_j) = (0, \ldots, 0)$, then we have

$$\begin{aligned} &x_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},0} \prod_{s=1}^{j-1} (x_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},s} \oplus y_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},n-s-1}) \\ &= x_{i^*,0} \prod_{s=1}^{j-1} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1. \end{aligned}$$

- If $(k_2,\ldots,k_j)\neq(0,\ldots,0)$, let l be the largest index such that $k_l=1$. Then from Property 2.1 we have

$$\begin{aligned}
&x_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},0}\prod_{s=1}^{j-1}(x_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},s}\oplus y_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},n-s-1})\\
&\quad=x_{i^*,0}\prod_{s=1}^{j-1}(x_{i^*,s}\oplus y_{i^*+k_2 2^{n-2}+\cdots+k_{l-1}2^{n-l+1}+2^{n-l},n-s-1})\\
&\quad=x_{i^*,0}(x_{i^*,l-1}\oplus y_{i^*,n-l}\oplus 1)\prod_{\substack{s=1\\ s\neq l-1}}^{j-1}(x_{i^*,s}\oplus y_{i^*+k_2 2^{n-2}+\cdots+k_{l-1}2^{n-l+1}+2^{n-l},n-s-1})=0.
\end{aligned}$$

In addition, by Property 2.1 we know that for any $(k_2,\ldots,k_j)\in\mathbb{F}_2^{j-1}$,

$$y_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},\frac{n}{2}-1}=x_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},\frac{n}{2}}=0$$

and

$$y_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j}+2^{n-1},\frac{n}{2}-1}=x_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j}+2^{n-1},\frac{n}{2}}=0.$$

Therefore, from (7b) we know that for any $(k_2,\ldots,k_j)\in\mathbb{F}_2^{j-1}$,

$$\eta_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j}}=\eta_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j}+2^{n-1}}=0.$$

Hence, we have

$$\bigoplus_{(k_2,\ldots,k_j)\in\mathbb{F}_2^{j-1}}(u_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j},j}\oplus u_{i^*+k_2 2^{n-2}+\cdots+k_j 2^{n-j}+2^{n-1},j})=1.$$

(ii) If $\frac{n}{2}+1<j<n$, then by Lemma 3.2(2d) and (8) we have

$$\begin{aligned}
&\bigoplus_{(k_2,\ldots,k_{j-n/2})\in\mathbb{F}_2^{j-n/2-1}}(u_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},j}\oplus u_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},j})\\
&=\bigoplus_{(k_2,\ldots,k_{j-n/2})\in\mathbb{F}_2^{j-n/2-1}}\Bigg(\xi_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}}\cdot\prod_{s=\frac{3n}{2}-j}^{n-2}(x_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},s}\\
&\quad\oplus y_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},n-s-1})\\
&\quad\oplus\eta_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}}\cdot\prod_{t=0}^{j-1}z_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},t}\\
&\quad\oplus\eta_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1}}\cdot\prod_{t=0}^{j-1}z_{i+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},t}\Bigg).
\end{aligned}$$

On the other hand, from Lemma 3.3(3b) we know there exists integer $i^* \geqslant 0$ such that

$$(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,0})(x_{i^*,\frac{n}{2}-1} \oplus y_{i^*,\frac{n}{2}} \oplus 1)(x_{i^*,0} \oplus y_{i^*,n-1}) \prod_{s=\frac{n}{2}+1}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

- If $(k_2, \ldots, k_{j-n/2}) = (0, \ldots, 0)$, similarly to (iv) in the proof of Theorem 3.1 we have

$$\xi_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}} \cdot \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},s}$$

$$\oplus\, y_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},n-s-1}) = \xi_{i^*} \cdot \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i^*,s} \oplus y_{i^*,n-s-1}) = 1.$$

- If $(k_2, \ldots, k_{j-n/2}) \neq (0, \ldots, 0)$, let l be the largest index such that $k_l = 1$. Then from Property 2.1 we have

$$\begin{aligned}
&\xi_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}} \cdot \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},s} \\
&\quad \oplus\, y_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},n-s-1}) \\
&= \xi_{i^*+k_2 2^{n-2}+\cdots+k_{l-1}2^{n-l+1}+2^{n-l}} \cdot \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i^*+k_2 2^{n-2}+\cdots+k_{l-1}2^{n-l+1}+2^{n-l},s} \oplus y_{i^*,n-s-1}) \\
&= \xi_{i^*+k_2 2^{n-2}+\cdots+k_{l-1}2^{n-l+1}+2^{n-l}} (x_{i^*,n-l} \oplus y_{i^*,l-1} \oplus 1) \\
&\quad \cdot \prod_{\substack{s=\frac{3n}{2}-j \\ s\neq n-l}}^{n-2} (x_{i^*+k_2 2^{n-2}+\cdots+k_{l-1}2^{n-l+1}+2^{n-l},s} \oplus y_{i^*,n-s-1}) \\
&= 0.
\end{aligned}$$

In addition, by Property 2.1 we know that for any $(k_2, \ldots, k_{j-n/2}) \in \mathbb{F}_2^{j-n/2-1}$,

$$x_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},\frac{n}{2}-1} \oplus y_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},\frac{n}{2}} = 0$$

and

$$x_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},\frac{n}{2}-1} \oplus y_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},\frac{n}{2}} = 0.$$

Similarly to (iv) in the proof of Theorem 4.1, for any $(k_2, \ldots, k_{j-n/2}) \in \mathbb{F}_2^{j-n/2-1}$,

- if $z_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},0} = 1$, then there exists integer $t_0 \in \{1, 2, \ldots, \frac{n}{2}-1\}$ such that

$$z_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},t_0} = 0;$$

- if $z_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},0}=0$, from (2a) we have $z_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},0}=1$, then there exists integer $t_1\in\{1,2,\ldots,\frac{n}{2}-1\}$ such that

$$z_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},t_1}=0.$$

Hence, we know that for any $(k_2,\ldots,k_{j-n/2})\in\mathbb{F}_2^{j-n/2-1}$,

$$\prod_{t=0}^{j-1} z_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},t}=\prod_{t=0}^{j-1} z_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},t}=0.$$

Thus

$$\bigoplus_{(k_2,\ldots,k_{j-n/2})\in\mathbb{F}_2^{j-n/2-1}} (u_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j},j}\oplus u_{i^*+k_2 2^{n-2}+\cdots+k_{j-n/2}2^{3n/2-j}+2^{n-1},j})=1.$$

From (i) and (ii) we have

$$(1\oplus x)^{\sum_{t=1}^{j}2^{n-t}}\underline{u}_j\neq\underline{0},\quad 1<j<\frac{n}{2}$$

and

$$(1\oplus x)^{\sum_{t=1}^{j-n/2}2^{n-t}}\underline{u}_j\neq\underline{0},\quad \frac{n}{2}+1<j<n.$$

Hence,

$$LC(\underline{u}_j)>\sum_{t=1}^{j}2^{n-t},\quad 1<j<\frac{n}{2}$$

and

$$LC(\underline{u}_j)>\sum_{t=1}^{j-n/2}2^{n-t},\quad \frac{n}{2}+1<j<n.$$

This completes the proof. □

5. Conclusions

In this paper, we propose two types of pseudorandom sequences based on single cycle T-functions, such that the periods of all their coordinate sequences can reach the maximal value 2^n. For the first proposal, the less significant half of the coordinate sequences are not cryptographically strong enough. Therefore, we improve it to obtain the second proposal. Experimental results indicate that all the coordinate sequences derived from the second proposal are almost uniformly distributed over $\mathbb{F}_2$, and their linear complexities are all close to their periods. How to provide other methods that equalize the periods of the coordinate sequences will be our future work.

Appendix A. Proof of Lemma 3.2

Proof. Since $\underline{\boldsymbol{x}} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ and $\underline{\boldsymbol{y}} = (\boldsymbol{y}_0, \boldsymbol{y}_1, \ldots)$ are two sequences over $\mathbb{Z}/(2^n)$ generated by single cycle T-functions $f(\boldsymbol{x})$ and $g(\boldsymbol{y})$, respectively, from Property 2.1 and Lemma 3.1 we know that

(i) If $j = 0$, then

$$z_{i,0} \oplus z_{i+2^{n-1},0} = x_{i,0} \oplus y_{i,n-1} \oplus x_{i+2^{n-1},0} \oplus y_{i+2^{n-1},n-1} = 1.$$

(ii) If $1 \leqslant j \leqslant \frac{n}{2} - 1$, then

$$\begin{aligned}
&z_{i,j} \oplus z_{i+2^{n-1},j} \\
&= x_{i,j} \oplus y_{i,n-j-1} \oplus x_{i+2^{n-1},j} \oplus y_{i+2^{n-1},n-j-1} \oplus \left(\bigoplus_{t=0}^{j-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{j-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\
&\quad \oplus \left(\bigoplus_{t=0}^{j-1} x_{i+2^{n-1},t} y_{i+2^{n-1},n-t-1} \prod_{s=t+1}^{j-1} (x_{i+2^{n-1},s} \oplus y_{i+2^{n-1},n-s-1}) \right) \\
&= \left(x_{i,0} y_{i,n-1} \prod_{s=1}^{j-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\
&\quad \oplus \left(x_{i+2^{n-1},0} y_{i+2^{n-1},n-1} \prod_{s=1}^{j-1} (x_{i+2^{n-1},s} \oplus y_{i+2^{n-1},n-s-1}) \right) \\
&= \left(x_{i,0} y_{i,n-1} \prod_{s=1}^{j-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \oplus \left(x_{i,0} (y_{i,n-1} \oplus 1) \prod_{s=1}^{j-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\
&= x_{i,0} \prod_{s=1}^{j-1} (x_{i,s} \oplus y_{i,n-s-1}).
\end{aligned}$$

(iii) If $j = \frac{n}{2}$, then

$$\begin{aligned}
&z_{i,\frac{n}{2}} \oplus z_{i+2^{n-1},\frac{n}{2}} \\
&= x_{i,n-1} \oplus y_{i,0} \oplus x_{i+2^{n-1},n-1} \oplus y_{i+2^{n-1},0} \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\
&\quad \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i+2^{n-1},t} y_{i+2^{n-1},n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i+2^{n-1},s} \oplus y_{i+2^{n-1},n-s-1}) \right) \\
&= 1 \oplus \left(x_{i,0} y_{i,n-1} \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\
&\quad \oplus \left(x_{i+2^{n-1},0} y_{i+2^{n-1},n-1} \prod_{s=1}^{\frac{n}{2}-1} (x_{i+2^{n-1},s} \oplus y_{i+2^{n-1},n-s-1}) \right)
\end{aligned}$$

$$= 1 \oplus \left(x_{i,0} y_{i,n-1} \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \oplus \left(x_{i,0} (y_{i,n-1} \oplus 1) \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right)$$

$$= 1 \oplus x_{i,0} \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}).$$

(iv) If $\frac{n}{2} + 1 \leqslant j \leqslant n$, then

$$\begin{aligned}
&z_{i,j} \oplus z_{i+2^{n-1},j} \\
&= x_{i,\frac{3n}{2}-j-1} \oplus y_{i,j-\frac{n}{2}} \oplus x_{i+2^{n-1},\frac{3n}{2}-j-1} \oplus y_{i+2^{n-1},j-\frac{n}{2}} \\
&\quad \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \prod_{s=\frac{3n}{2}-j}^{n-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \\
&\quad \oplus \left(\bigoplus_{t=0}^{\frac{n}{2}-1} x_{i+2^{n-1},t} y_{i+2^{n-1},n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i+2^{n-1},s} \oplus y_{i+2^{n-1},n-s-1}) \right. \\
&\quad \left. \cdot \prod_{s=\frac{3n}{2}-j}^{n-1} (x_{i+2^{n-1},s} \oplus y_{i+2^{n-1},n-s-1}) \right) \oplus \left(\bigoplus_{t=0}^{j-\frac{n}{2}-1} x_{i,n-t-1} y_{i,t} \prod_{s=t+1}^{j-\frac{n}{2}-1} (x_{i,n-s-1} \oplus y_{i,s}) \right) \\
&\quad \oplus \left(\bigoplus_{t=0}^{j-\frac{n}{2}-1} x_{i+2^{n-1},n-t-1} y_{i+2^{n-1},t} \prod_{s=t+1}^{j-\frac{n}{2}-1} (x_{i+2^{n-1},n-s-1} \oplus y_{i+2^{n-1},s}) \right) \\
&= \left\{ \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i,s} \oplus y_{i,n-s-1}) (x_{i,n-1} \oplus y_{i,0}) \right. \\
&\quad \left. \cdot \left[\left(x_{i,0} y_{i,n-1} \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \oplus \left(\bigoplus_{t=1}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \right] \right\} \\
&\quad \oplus \left\{ \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i,s} \oplus y_{i,n-s-1}) (x_{i,n-1} \oplus y_{i,0} \oplus 1) \right. \\
&\quad \left. \cdot \left[\left(x_{i,0} (y_{i,n-1} \oplus 1) \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \right. \right. \\
&\quad \left. \left. \oplus \left(\bigoplus_{t=1}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \right] \right\} \\
&\quad \oplus \left(x_{i,n-1} y_{i,0} \prod_{s=1}^{j-\frac{n}{2}-1} (x_{i,n-s-1} \oplus y_{i,s}) \right) \oplus \left((x_{i,n-1} \oplus 1) y_{i,0} \prod_{s=1}^{j-\frac{n}{2}-1} (x_{i,n-s-1} \oplus y_{i,s}) \right)
\end{aligned}$$

$$= \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i,s} \oplus y_{i,n-s-1}) \cdot \left\{ \left(x_{i,0}(x_{i,n-1} \oplus y_{i,n-1} \oplus y_{i,0} \oplus 1) \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \right.$$

$$\left. \oplus \left(\bigoplus_{t=1}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \right\} \oplus \left(y_{i,0} \prod_{s=1}^{j-\frac{n}{2}-1} (x_{i,n-s-1} \oplus y_{i,s}) \right)$$

$$= \prod_{s=\frac{3n}{2}-j}^{n-2} (x_{i,s} \oplus y_{i,n-s-1}) \cdot \left\{ \left(x_{i,0}(x_{i,n-1} \oplus y_{i,n-1} \oplus y_{i,0} \oplus 1) \prod_{s=1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \right.$$

$$\left. \oplus \left(\bigoplus_{t=1}^{\frac{n}{2}-1} x_{i,t} y_{i,n-t-1} \prod_{s=t+1}^{\frac{n}{2}-1} (x_{i,s} \oplus y_{i,n-s-1}) \right) \oplus y_{i,0} \right\}.$$

This proves the lemma. □

Appendix B. Proof of Lemma 3.3

Proof. We first show that the equality (3a) holds, and the other two equalities can be shown in a similar way.

Since $per(\underline{x}_0) = 2$, there exists $i_1 \geqslant 0$ such that $x_{i_1,0} = 1$. Moreover, from Property 2.1 we know that $x_{i_1+2^j,0} = 1$ also holds for all $j \geqslant 1$.

If $\prod_{s=1}^{\frac{n}{2}-1} (x_{i_1,s} \oplus y_{i_1,n-s-1}) = 1$, then set $i^* = i_1$. Hence, the result holds. Otherwise, let s_1 be the largest integer $s \in \{1, 2, \ldots, \frac{n}{2} - 1\}$ such that $x_{i_1,s} \oplus y_{i_1,n-s-1} = 0$. Then we have

$$x_{i_1,s_1} \oplus y_{i_1,n-s_1-1} = 0 \quad \text{and} \quad x_{i_1,s} \oplus y_{i_1,n-s-1} = 1, \quad s_1 < s \leqslant \frac{n}{2} - 1.$$

Set $i_2 = i_1 + 2^{n-s_1-1}$. Then from Property 2.1 we know that

$$\begin{aligned} &x_{i_2,0} = x_{i_1,0} = 1, \\ &x_{i_2,s_1} \oplus y_{i_2,n-s_1-1} = x_{i_1,s_1} \oplus (y_{i_1,n-s_1-1} \oplus 1) = 1, \quad \text{and} \\ &x_{i_2,s} \oplus y_{i_2,n-s-1} = x_{i_1,s} \oplus y_{i_1,n-s-1} = 1, \quad s_1 < s \leqslant \frac{n}{2} - 1. \end{aligned}$$

That is,

$$x_{i_2,0} = 1 \quad \text{and} \quad \prod_{s=s_1}^{\frac{n}{2}-1} (x_{i_2,s} \oplus y_{i_2,n-s-1}) = 1.$$

If $\prod_{s=1}^{s_1-1} (x_{i_2,s} \oplus y_{i_2,n-s-1}) = 1$, then set $i^* = i_2$. Hence, the result holds. Otherwise, let s_2 be the largest integer $s \in \{1, 2, \ldots, s_1 - 1\}$ such that $x_{i_2,s} \oplus y_{i_2,n-s-1} = 0$. Set $i_3 = i_2 + 2^{n-s_2-1}$. Similarly we have

$$x_{i_3,0} = 1 \quad \text{and} \quad \prod_{s=s_2}^{\frac{n}{2}-1} (x_{i_3,s} \oplus y_{i_3,n-s-1}) = 1.$$

Therefore, if $\prod_{s=1}^{s_2-1}(x_{i_3,s} \oplus y_{i_3,n-s-1}) = 1$, then set $i^* = i_3$. Hence, the result holds. Otherwise, repeat the above process.

Since $1 \leqslant s_2 < s_1 \leqslant \frac{n}{2} - 1$ and the set $\{1, 2, \ldots, \frac{n}{2} - 1\}$ contains finite number of integers, by recursive analysis we know there exists strictly decreasing integer series $\{s_0 = \frac{n}{2}, s_1, s_2, \ldots, s_l\}$ such that

$$x_{i_{k+1},0} = 1, \qquad \prod_{s=s_k}^{\frac{n}{2}-1}(x_{i_{k+1},s} \oplus y_{i_{k+1},n-s-1}) = 1, \quad \text{and} \quad \prod_{s=1}^{s_l-1}(x_{i_{l+1},s} \oplus y_{i_{l+1},n-s-1}) = 1$$

hold for all $1 \leqslant k \leqslant l$, where s_k is the largest integer $s \in \{1, 2, \ldots, s_{k-1} - 1\}$ such that $x_{i_k,s} \oplus y_{i_k,n-s-1} = 0$ and $i_{k+1} = i_k + 2^{n-s_k-1}$. Let $i^* = i_{l+1}$. Then the result holds. □

References

[1] A. Klimov, A. Shamir, A new class of invertible mappings, in: Workshop on Cryptographic Hardware and Embedded Systems—CHES 2002, in: Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, Berlin, 2003, pp. 470–483.

[2] A. Klimov, A. Shamir, Cryptographic applications of T-functions, in: Workshop on Selected Areas in Cryptography—SAC 2003, in: Lecture Notes in Comput. Sci., vol. 3006, Springer-Verlag, Berlin, 2004, pp. 248–261.

[3] A. Klimov, A. Shamir, New cryptographic primitives based on multiword T-functions, in: Fast Software Encryption—FSE 2004, in: Lecture Notes in Comput. Sci., vol. 3017, Springer-Verlag, Berlin, 2004, pp. 1–15.

[4] A. Klimov, A. Shamir, New applications of T-functions in block ciphers and hash functions, in: Fast Software Encryption—FSE 2005, in: Lecture Notes in Comput. Sci., vol. 3557, Springer-Verlag, Berlin, 2005, pp. 18–31.

[5] A. Klimov, Applications of T-functions in cryptography, PhD dissertation, Weizmann Institute of Science, Rehovot, Israel, 2005.

[6] J. Hong, D.H. Lee, Y. Yeom, D. Han, T-function based stream cipher TSC-3, ECRYPT Stream Cipher Project Report 2005/031, 2005, http://www.ecrypt.eu.org/stream.

[7] D. Moon, D. Kwon, D. Han, J. Lee, T-function based stream cipher TSC-4, ECRYPT Stream Cipher Project Report 2006/024, 2006, http://www.ecrypt.eu.org/stream.

[8] V. Anashin, A. Bogdanov, I. Kizhvtov, S. Kumar, ABC: A new fast flexible stream cipher, ECRYPT Stream Cipher Project Report 2005/001, 2005, http://www.ecrypt.eu.org/stream.

[9] A. Maximov, A new stream cipher "Mir-1", ECRYPT Stream Cipher Project Report 2005/017, 2005, http://www.ecrypt.eu.org/stream.

[10] J. Mitra, P. Sarkar, Time-memory trade-off attacks on multiplications and T-functions, in: Advances in Cryptology—ASIACRYPT 2004, in: Lecture Notes in Comput. Sci., vol. 3329, Springer-Verlag, Berlin, 2004, pp. 468–482.

[11] N. Kolokotronis, Cryptographic properties of stream ciphers based on T-functions, in: IEEE International Symposium on Information Theory—ISIT 2006, 2006, pp. 1604–1608.

[12] K.J. Xu, Z.P. Dai, Z.D. Dai, The formulas for the coefficients of the sum and product of p-adic integers with applications to Witt vectors, Acta Arith. 150 (4) (2011) 361–384.